A RATIONAL REPRESENTATION OF CODES AND (L, g)-CODES

V. D. Goppa

UDC 621.391.152

A method of construction of error-correcting codes is described as well as a class of linear q-ary codes.

1. Introduction

This paper generalizes the results set forth by the author in [1]. At the beginning we describe a method of construction of error-correcting codes that makes it possible to interpret a linear q-ary code of weight d as a set of rational functions of degree $\geq d$. The possibilities of the method are illustrated by the construction of a wide class of codes called (L, g)-codes. The codes have the following parameters: $n \leq q^m$, $k \geq n - 2mt$, and $d \geq 2t + 1$. The decoding of these codes is not more complicated than the decoding of Bose–Chaudhuri–Hocquenghem (BCH) codes; for some (L, g)-codes there exist also simpler decoding schemes. In conclusion we shall consider some particular cases of (L, g)-codes, and we shall study their behaviour for $n \to \infty$.

2. Rational Representation of Codes

1. Principal Isomorphism. Let $q = p^l$, p is a prime, $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, $n \leq q^m$, $\alpha_i \in GF(q^m)$, $\alpha_i \neq \alpha_j$, with $GF(q^m)$, being the minimal field containing L, S is a vector space over GF(q) of dimension n, S_H is a metric space S with a Hamming norm, and R a vector space of rational functions over $GF(q^m)$ of the form

$$\xi(z) = \sum_{i=1}^{n} \frac{b_i}{z - \alpha_i}, \quad b_i \in GF(q), \quad \alpha_i \in L. \tag{1}$$

Let us introduce a norm in R as follows: for any irreducible fraction

$$\xi(z) = \frac{\psi(z)}{\varphi(z)} \in R, \quad \xi \neq 0, \quad \|\xi(z)\| = \deg \varphi(z). \tag{2}$$

By R_d we shall denote a space R that has been metricized with the aid of this norm. Let $x \in S$, $x = (b_1, b_2 \ldots, b_n)$.

The mapping $x \to \xi_x(z) = \sum_{i=1}^{n} b_i/(z - \alpha_i)$ is an isomorphism of S onto R. Since $\xi_x(z) = \|x\|$, this mapping will be an isometry of S_H onto R_d, i.e., $S_H \approx R_d$. This isomorphism makes it possible to define codes as subsets of R. In particular, a linear code of weight d is a linear subspace of R consisting of fractions of degree not smaller than d.

2. Characterization of R for a Prime q. If q is a prime, then GF(q) will coincide with the residue field Z_q of integers modulo-q, and it will be useful to characterize the elements of R as follows.

To each vector $x \in S$, $x = (b_1, b_2, \ldots, b_n)$ we assign a polynomial $f_x(z) = (z-\alpha_1)^{b_1}(z-\alpha_2)^{b_2}\ldots(z-\alpha_n)^{b_n}$. Then any fraction $\xi \in R$ can be represented in the form $\xi = f_x'/f_x$, where $x \in S$ and f_x' is the formal derivative of the polynomial f_x.

3. Construction of Binary Codes. For the construction of binary codes it is possible to use a more general procedure. Let S be a vector space of dimension n over GF(2), K an integer domain with unity,

Translated from Problemy Peredachi Informatsii, No. 3, pp. 41-49, July-September, 1971. Original article submitted February 27, 1970.

L a set of n distinct elements K: $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, D a multiplicative monoid of polynomials over K with roots in L, and D^2 a submonoid of D consisting of polynomials with roots of even multiplicity.

Two polynomials in D that differ by a factor belonging to D^2 will be assumed equivalent. A factor monoid D/D^2 with respect to this equivalence relation is a multiplicative group. As representatives of equivalence classes we shall take polynomials of smallest degree in a class. Such a representative can be obtained from any polynomial $f \in D$ by reduction modulo-2 of all the multiplicities of the roots of this polynomial.

Let $x \in S$. The correspondnece $x \to f_x(z)$ is an isomorphism of the additive group S onto the multiplicative group D/D^2: $S \approx D/D^2$. Here $\deg f_x(z) = d$ if the weight of x is equal to d. By using this isomorphism, it is possible to define a linear binary code of weight d as a multiplicative subgroup of the group D/D^2 consisting of polynomials of degree not smaller than d.

For obtaining such a code, it suffices to specify a monoid F such that $D^2 \subset F \subset D$. Then the linear code C will be equal to F/D^2. Let us point out the wide possibilities of such a method of code construction. Binary codes are defined with the aid of polynomials over an arbitrary integer domain (in particular, it is possible to use real polynomials), and the weight of the code vector is determined on the basis of the degree of the polynomial.

By taking $K = GF(2^m)$, we obtain $f'(z) = 0$ for any $f \in D^2$. Since for any $\varphi, \psi \in D/D^2$ we have $(\varphi\psi)'/\varphi\psi = \varphi'/\varphi + \psi'/\psi$, it follows that in this case D/D^2 will be isomorphic to an additive group R of functions of the form φ'/φ, and we obtain the principal isomorphism.

3. (L, g)-Codes

1. Definition. Estimation of Weight and Power. We shall use the principal isomorphism for defining a wide class of linear codes. Let g(z) be a polynomial over $GF(q^m)$ that has no roots in L. For any $\xi(z) = \psi(z)/\varphi(z) \in R$ the polynomial $\varphi(z)$ is relatively prime to g(z), and hence invertible in the algebra G of polynomials modulo-g. Let us define an (L, g)-code as a set of elements $\xi(z) \in R$ such that $\xi(z) \equiv 0 \bmod g(z)$.

The linearity of such a code is evident. Estimates of the weight and power are presented in the following theorems.

THEOREM 1. An (L, g)-code has not more than $m \cdot \deg g(z)$ check symbols.

Proof. By definition, an (L, g)-code is the kernel of a linear mapping of the space R into an algebra G of polynomials modulo g(z). Thus the number of check symbols coincides with the dimension over GF(q) of the image of R under this mapping, and this dimension cannot be larger than $m \cdot \deg g$ (the dimension of the algebra).

THEOREM 2. The weight of any element of an (L, g)-code is not smaller than $\deg g + 1$.

Proof. If $\xi \equiv 0 \bmod g$ and $\xi \equiv \psi/f$, then $\psi \equiv 0 \bmod g$, i.e., $\deg \psi \geq \deg g$, and hence $\deg \xi \geq \deg g + 1$, which completes the proof.

For $q \neq 2$, (L, g)-codes will be more effective that have a check matrix with an additional row of ones (modified (L, g)-codes).

THEOREM 3. The parameters of a modified (L, g)-code satisfy the conditions $n \leq q^m$, $k \geq n - (2t-1)m - 1$, $d \geq 2t + 1$.

Proof. Let $x \in S$, $x = (b_1, b_2, \ldots, b_n)$ be a code vector. Then $\xi = \psi/\varphi \equiv 0 \bmod g$, $\sum_1^n b_i = 0$. Since the leading coefficient of the polynomial ψ is $\sum_1^n b_i$, it follows that $\deg \varphi \geq \psi + 2 \geq \deg g + 2$.

Hence for the correction of t errors it suffices to take a polynomial g such that $\deg g = 2t-1$.

2. The Check Matrix. In connection with (L, g)-codes there appears a new form of check matrix, i.e., the check matrix is in the form of a row of polynomials (a check matrix of compact form). Such a form is convenient in the analysis of the properties of a code and in the construction of decoding schemes. The check matrix of (L, g)-codes can be represented in the following forms.

First compact form:

$$T_{1c} = \left\| \frac{g(z) - g(\alpha_1)}{z - \alpha_1} g^{-1}(\alpha_1) \dots \frac{g(z) - g(\alpha_n)}{z - \alpha_n} g^{-1}(\alpha_n) \right\|;$$

second compact form:

$$T_{2c} = \left\| \frac{z^r - \alpha_1^r}{z - \alpha_1} g^{-1}(\alpha_1) \dots \frac{z^r - \alpha_n^r}{z - \alpha_n} g^{-1}(\alpha_n) \right\|.$$

Here r = deg g(z).

Expanded form:

$$T_e = \begin{Vmatrix} g^{-1}(\alpha_1) & \dots & g^{-1}(\alpha_n) \\ g^{-1}(\alpha_1)\alpha_1 & \dots & g^{-1}(\alpha_n)\alpha_n \\ \dots & \dots & \dots \\ g^{-1}(\alpha_1)\alpha_1^{r-1} & \dots & g^{-1}(\alpha_n)\alpha_n^{r-1} \end{Vmatrix}.$$

We can convince ourselves of the validity of these forms in the same way as in [1].

Thus the check matrix of an (L, g)-code can be obtained from a "rectangular Vandermonde matrix" by multiplying the columns by the elements $g^{-1}(\alpha_i)$. It is possible to define more general codes by taking as factors any nonzero elements not necessarily equal to $g^{-1}(\alpha_i)$. As before, any r columns of the thus-obtained matrix will be linearly independent over GF(q^m); therefore the weight of the code will be larger than r.

By taking as factors the elements $g^{-1}(\alpha_i)$, we obtain the definition of (L, g)-codes given at the beginning of § 3, and we can estimate the parameters with the aid of more refined methods, not related to the check matrix (Theorems 1 and 2). Thus if q = 2 and g does not have multiple roots, then the weight of any code element will be larger than 2r; in this case the check matrix T_p will yield a bound that is larger than r only.

3. Decoding. Let y = x + e, with y, x, e $\in$ S, and let x be the transmitted code vector and e the error vector with nonzero coordinates $b_{i_1}, b_{i_2}, \dots, b_{i_k}$, $k \le t$. By multiplying the vector y by the matrix $\overset{k}{T}_{1k}'$ (the transpose of T_{1k}), we obtain the syndrome $S(z) = \sum_{l=1}^{k} b_{il} [(g(z) - g(\alpha_{il})]/(z - \alpha_{il}) g^{-1}(\alpha_{il})$. Let $\psi/f = -\sum_{l=1}^{k} b_{il}/(z - \alpha_{il})$. Then

$$fS \equiv \psi \bmod g, \ \deg f \leqslant t, \ \deg \psi < t, \tag{3}$$

and for decoding it suffices to solve the congruence (3) for f and ψ.

THEOREM 4. If deg g = 2t, then for any polynomoal S(z) of degree < 2t the set D of pairs (u, v) such that $uS \equiv v \bmod g$, deg u $\le$ t, deg v < t will contain a nonzero element. All the pairs (u, v) belonging to D will have the same ratio $v/u = \eta$.

Proof. Let A be a linear operator of multiplication by S in the coset algebra of polynomials modulo g(z). In the basis $1, z, \dots, z^{2t-1}$ the matrix of this operator has the form

$$A = \begin{Vmatrix} c_{2t-1\,0} & \dots & c_{2t-1\,2t-1} \\ \dots & \dots & \dots \\ c_{00} & \dots & c_{0\,2t-1} \end{Vmatrix}, \text{ where } z^j S(z) = \sum_{i=0}^{2t-1} c_{ij} z^i, \ j = 0, 1, \dots, 2t-1.$$

Let us denote by $A_{t, t+1}$ the submatrix of A constructed from t upper rows and the first t + 1 columns. The equation

$$A_{t, t+1} x = 0 \tag{4}$$

always has a solution, whence follows the existence of a quanitity u that satisfies the condition of the theorem and also its method of determination.

Now let (u_1, v_1), $(u_2, v_2) \in D$. Then $u_1 \overline{S} \equiv \overline{v}_1 \bmod \overline{g}$, $\overline{v}_2 \equiv \overline{S} u_2 \bmod \overline{g}$, where the polynomials $\overline{S}$, $\overline{v}_1$, $\overline{v}_2$ and $\overline{g}$ were obtained from S, v_1, v_2 and g by division by the largest common divisor of S and g. Since $\overline{S}$ and $\overline{g}$ are relatively prime, it follows that $u_1 \overline{v}_2 \equiv \overline{v}_1 u_2 \bmod g$, $u_1 \overline{v}_2 - \overline{v}_1 u_2 \equiv 0 \bmod g$, and since the degree of the polynomial in the left-hand side is smaller than the degree of $\overline{g}$, it follows that $\overline{v}_1/u_1 = \overline{v}_2/u_2$, so that $v_1/u_1 = v_2/u_2$, which completes the proof.

From this theorem we obtain the following rule of decoding of (L, g)-codes: 1) Find a syndrome S(z); 2) find a solution u of system (4); 3) calculate $v \equiv u \cdot S \bmod g$; 4) find $\eta = v/u$ (this ratio will coincide in the case under consideration with ψ/f from the congruence (3), since f and ψ are relatively prime); 5) decompose η into simple fractions (for this purpose it is necessary to find the roots of f(z) and calculate $c_{il} = \psi(\alpha_{il})/f'(\alpha_{il})$); 6) determine the values of the errors: $b_{il} = -c_{il}$.

Another method of decoding involves the use of the check matrix T_{2C}. By multiplying the vector y by the matrix T_{2C}' we obtain the syndrome $S(z) = \sum b_{il}(z^r - \alpha_{il}^r)/(z-\alpha_{il})\, g^{-1}(\alpha_{il})$. Let

$$\frac{\psi}{f} = -\sum_{l=1}^{k} b_{i_l} \frac{\alpha_{i_l}^r}{z-\alpha_{i_l}} g^{-1}(\alpha_{i_l}).$$

Then the decoding reduces to solving the congruence

$$f \cdot S \equiv \psi \bmod z^r \tag{5}$$

for $\alpha_{il} \neq 0, l = 1, 2, \ldots, k$, or the congruence

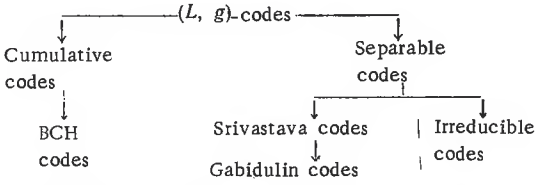
$$f \cdot S \equiv \psi \bmod z^{r-1} \tag{6}$$

for $\alpha_{ij} = 0$ for some j.

In the first case deg f = k, and in the second case deg f = k−1, so that for r = 2t there exists by virtue of Theorem 4 a unique solution (f, ψ) of the congruence (5) with f and ψ being relatively prime, deg f ≤ t, deg ψ < t, or of the congruence (6) with f and ψ being relatively prime, deg f ≤ t−1, deg ψ < t−1.

Berlekamp (2) has proposed an iterative decoding procedure for BCH codes that is in fact a method of solution of the congruence (5). The procedure involves successive transition from a congruence modulo z^2 to a congruence modulo z^3, then to a congruence modulo z^4, etc. The Berlekamp algorithm saves a large amount of equipment, since it does not require storage of the matrix $A_{t,t+1}$.

5. Special (L, g)-Codes. Below we shall consider some particular (L, g)-codes that are related as follows:



The classification is based on the form of the generating polynomial. Cumulative codes are of the same type as BCH codes. Separable codes have a peculiar decoding scheme. For both these classes of codes it is possible to improve the parameter bounds in the binary case: $n \leq 2^m$, $k \geq n - mt$, $d \geq 2t + 1$.

The Srivastava codes and the Gabidulin codes were obtained in 1967. Irreducible codes have the "strongest" algebraic structure, and we have the impression that in studying the properties of these codes it is possible to make good progress.

4. Cumulative Codes

Cumulative codes are codes whose generating polynomial has one root: $g(z) = (z-\alpha)^r$.

The maximal L that can be taken for such codes corresponds to $GF(q^m) - \{\alpha\}$, so that their maximal length is equal to $q^m - 1$. A particular case of such codes for $g(z) = z^r$ is BCH codes (with such a choice of g(z) the parity check matrix T_e goes over into the well-known parity check matrix for a BCH code).

THEOREM 5. All the cumulative codes with the same r have the same spectrum.

Proof. If x is an element of a $(GF(q^m) - \{\alpha\}, (z-\alpha)^r)$-code, then $\xi_x(z) = \psi(z)/\varphi(z) \equiv 0 \bmod (z-\alpha)^r$, so that

$$\frac{\psi(z+\alpha)}{\varphi(z+\alpha)} \equiv 0 \bmod z^r.$$

If $\varphi(z)$ has roots $\alpha_{i_1}, \ldots, \alpha_{il}$, then $\varphi(z+\alpha)$ will have roots $\alpha_{i_1} - \alpha, \ldots, \alpha_{il} - \alpha$ that lie in $GF(q^m) - \{0\}$. Thus there exists a weight-preserving one-to-one correspondence between any cumulative code and a BCH code.

THEOREM 6. BCH codes are the only cyclic (L, g)-codes with $L = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, where α is the n-th primitive root of unity.

Proof. With such a choice of L it is possible to characterize cyclic codes with the aid of a rational representation as follows: a cyclic code is a set of fractions in R (§ 2) that form a linear space, this set being closed under the substitution $z \to \alpha z$, $\alpha \in L$: $C = \{\xi(z) \in R: \xi(\alpha z) \in C, a \in L\}$. We shall assume that the generating polynomial g(z) of a cyclic (L, g)-code has a nonzero root β. Any $\xi(z)$ belonging to this code satisfies the congruence

$$\xi(\alpha z) = \frac{\psi(\alpha z)}{\varphi(\alpha z)} \not\equiv 0 \bmod g(z)$$

for all $\alpha \in L$; this signifies that $\psi(z)$ has in addition to the root β all the other roots of the form $\alpha\beta$, i.e., $\deg \psi(z) \geq n$, which is impossible. Hence $g(z) = z^r$.

5. Separable Codes

1. Definition. Check Matrix. Separable codes are codes whose generating polynomial does not have multiple roots:

$$g(z) = (z - z_1)(z - z_2) \ldots (z - z_r).$$

Binary separable codes, just as BCH codes, admit an improvement in their parameter bounds. Indeed, in accordance with § 2.2 we have $f'/f \equiv 0 \bmod g$, and since the derivative in a field of characteristic 2 is a square, it follows that $f'/f \equiv 0 \bmod g^2$. Hence for $\deg g = t$ we have $n \leq 2^m$, $k \geq n - mt$, $d \geq 2t + 1$. Separable codes have the following specific form of the check matrix (Cauchy matrix): $T_c = \| (z_i - \alpha_j)^{-1} \|$, $i = 1, 2, \ldots, r$, $j = 1, 2, \ldots, n$, where z_i and α_j are distinct elements of the field $GF(q^m)$ or of an extension of this field. By using the check matric T_c we obtain an efficient decoding method for such codes based on rational interpolation.

2. Decoding. Let y, x and e be the same as in § 3.3. By multiplying the vector y by the matrix T_c', we obtain a syndrome $(\xi_1, \xi_2, \ldots, \xi_r)$, where $\xi_i = \xi(z_i)$,

$$\xi(z) = \sum_{l=1}^{k} \frac{b_{i_l}}{z - \alpha_{i_l}}. \tag{7}$$

In this case decoding involves the reconstruction of the fraction $\xi(z)$ on the basis of its values at certain points (rational interpolation [3]).

Let K be a field and $\xi(z) = \psi(z)/f(z)$ an irreducible fraction over the field K, $\deg f = n$, $\deg \psi \neq m$. The order of a fraction is defined as a quantity $r(\xi)$ equal to $2n$ for $m \leq n$, and to $2n-1$ for $m > n$. Any irreducible rational fraction of order $\leq k$ can be uniquely reconstructed on the basis of its values at the $(k+1)$-th point of the field K.

THEOREM 7. Let $z_1, z_2, \ldots, z_{k+1}$ be distinct elements of the field K. Any irreducible fraction $\psi(z)/f(z) = \xi(z) \in K(z)$ of order $r \leq k$ can be represented in the form

$$\xi(z) = \lambda_1 + \cfrac{z - z_{i_1}}{\lambda_2 + \cfrac{z - z_{i_{r-1}}}{\lambda_r}}, \tag{8}$$

$$z_{i_1} \neq z_{i_2} \neq \ldots \neq z_{i_{r-1}}.$$

Proof. Among the elements $z_1, z_2, \ldots, z_{k+1}$ there exists an element z_{i_l} such that $f(z_{i_l}) \neq 0$. Let us write $\lambda_1 = \xi(z_{i_l})$. Then

$$\xi(z) = \lambda_1 + \frac{z - z_{i_1}}{\xi_1(z)}, \text{ where } \xi_1(z) = \frac{f(z)}{\psi_1(z)}, \ \psi_1(z) = \frac{\psi(z) - \lambda_1 f(z)}{z - z_{i_1}}.$$

If $m \leq n$, then $r(\xi) = 2n$, $\deg \psi < n$, $r(\xi_1) = 2n-1$. If $m > n$, then $r(\xi) = 2m-1$, $\deg \psi_1 = m-1$, $r(\xi_1) = 2m-2$. Hence we have in any case $r(\xi_1) = r(\xi) - 1$. By applying the previous reasoning to the fraction $\xi_1(z)$, then to the fraction $\xi_2(z)$, etc., we obtain the decomposition (8) after precisely r steps.

The quantities $\lambda_1, \lambda_2, \ldots, \lambda_r$ in (8) are determined by successive substitution $z = z_{i_1}$, $z = z_{i_2}$, etc. It is convenient to perform the calculations by the scheme

$$\begin{array}{lllll} z_1 & y_1^{(1)} & & & \\ z_2 & y_2^{(1)} & y_1^{(2)} & & \\ z_3 & y_3^{(1)} & y_2^{(2)} & y_1^{(3)} & \\ z_4 & y_4^{(1)} & y_3^{(2)} & y_2^{(3)} & y_1^{(4)} \\ z_5 & y_5^{(1)} & y_4^{(2)} & y_3^{(3)} & y_2^{(4)} \quad y_1^{(5)} \end{array} \tag{9}$$

Here

$$y_i^{(1)} = y_i = \xi(z_{i-1}),$$

$$y_i^{(j)} = \frac{z_{i+j-1} - z_{j-1}}{y_{i+1}^{(j-1)} - y_1^{(j-1)}}, \ j > 1.$$

If $y_{i+1}^{(j)} = y_1^{(j)}$ for some $i \neq 0$, then the $(i+1)$-th row must be eliminated from (9). The quantities λ_1, $\lambda_2, \ldots, \lambda_r$ form the upper diagonal in (9), i.e., $\lambda_j = y_1^{(j)}$. Instead of (9) it is possible to construct inverse differences and then use them for determining λ_j:

$$\begin{array}{llll} z_1 & y_1 & & \\ z_2 & y_2 & \rho_1(z_2z_1) & \\ z_3 & y_3 & \rho_1(z_3z_2) & \rho_2(z_3z_2z_1) \\ z_4 & y_4 & \rho_1(z_4z_3) & \rho_2(z_4z_3z_2) \end{array} \qquad \rho_3(z_4z_3z_2z_1) \tag{10}$$

Here $\rho_1(z_2z_1) = z_2 - z_1/y_2 - y_1$,

$$\rho_2(z_3z_2z_1) = \frac{z_3 - z_1}{\rho_1(z_3z_2) - \rho_1(z_2z_1)} + y_2 \text{ etc.}$$

In terms of inverse differences the quantities λ_j are defined as follows:

$$\lambda_j = \rho_j(z_{j+1}z_j \ldots z_1) - \rho_{j-2}(z_{j-1}z_{j-2} \ldots z_1)$$

for $j > 2$ and $\lambda_1 = y_1$, $\lambda_2 = \rho_1(z_2z_1)$. The inverse differences $\rho_j(z_{j+1} \ldots z_1)$ are symmetrical in all the variables.

If $q \neq 2$, deg $g = 2t$, $k \leq t$, then the fraction $\xi(z)$ (7) will have an order $\leq 2t$ and it can be uniquely reconstructed on the basis of its values at $2t + 1$ points. If $q = 2$, deg $g = t$ and $k \leq t$, we must effect the following transformations:

$$f(z) = u^2(z) + zv^2(z), \quad v^2 = f', \quad f(z_i)\xi_i = f'(z_i),$$
$$u^2(z_i)\xi_i = v^2(z_i)(1 + z_i\xi_i).$$

If $\xi_i = 0$, then z_i will be a root of $v^2(z)$, and if $1 + z_i\xi_i = 0$, then z_i will be a root of $u^2(z)$. Knowing the values of $y_i = u(z_i)/v(z_i) = \sqrt{z_i + \xi^{-1}}$ at points z_i at which $\xi_i \neq 0$, it is possible to uniquely reconstruct $u(z)/v(z)$ by representing it in the form of a continued fraction (8).

3. Srivastava Codes. These are codes whose generating polynomial decomposes in a minimal field containing L. Such codes are described in [2], where their decoding scheme (based on rational interpolation) is also mentioned. Srivastava codes have the following bounds:

$$n \leqslant q^m - 2t, \quad k \geqslant n - 2mt, \quad d \geqslant 2t + 1.$$

4. Gabidulin Codes. A particular case of Srivastava codes (for $m = 1$) was independently obtained by Gabidulin [4] who also noted that if Cauchy's matrix (in the case that $L \subset GF(g)$) is augmented by the unit matrix, the code weight will not decrease. Maximal codes defined by such a parity check matrix yield a higher rate of transmission than Reed–Solomon codes, i.e. $n = q$, $k = n - 2t$, $d = 2t + 1$.

5. Irreducible Codes. A separable code is said to be irreducible if the polynomial $g(z)$ is irreducible over a minimal field containing L.

The parity check matrix of an irreducible code consists of the row

$$T_{\text{II}} = ((z_0 - \alpha_1)^{-1}(z_0 - \alpha_2)^{-1} \ldots (z_0 - \alpha_n)^{-1}),$$

where Z_0 is a root of $g(z)$. The value of a rational function over $GF(q^m)$ at a point $z_0 \in GF(q^{mr})$ determines the value of this function at points conjugate to z_0 over the field $GF(q^m)$:

$$\xi(z_0) = y_0, \quad \xi(\sigma z_0) = \sigma y_0, \ldots, \quad \xi(\sigma^{r-1}z_0) = \sigma^{r-1}y_0.$$

All the inverse differences of the same order, calculated for the points $z_0, \sigma z_0, \ldots, \sigma^{r-1}z_0$, will be conjugate:

$$\begin{array}{llll} z_0 & y_0 & \rho_1 & \\ \sigma z_0 & \sigma y_0 & \sigma\rho_1 & \rho_2 \\ \sigma^2 z_0 & \sigma^2 y_0 & \sigma^2\rho_1 & \sigma\rho_2 \\ \sigma^3 z_0 & \sigma^3 y_0 & & \end{array} \qquad \rho_3$$

Hence for the decoding of irreducible codes it is not necessary to construct the entire table of inverse differences. It is apparently simpler to perform stage-by-stage decoding of such codes. The number of errors for a syndrome y_0 can be determined by the following algorithm (here σ is the generatrix of the Galois group of the field $GF(q^{mr})$ over the field $GF(q^m)$ and the notation A: = B has the same meaning as in ALGOL, i.e., assign to A the value B): For $q \neq 2$: 1° write A: = z_0; C: = 0; D: = y_0; N: = 1; 2° calculate E: = σD − D; 3° if E: = 0, go to 5°; 4° write B: = σB; E: = (B − A)/(E + C); C: = σD; D: = E; N: = N + 1; go to 2°; 5° print the value of the number of errors equal to N/2; for $q = 2$: 1° write A: = B: = z_0; C = 0; D: = y_0; N: = 1; 2° calculate D: = $\sqrt{D^{-1} + A}$; 3° calculate E: = σD − D; 4° if E = 0, go to 6°; 5° write B: = σB; E: = (B − A)/(E + C); C: = σD; D: = E; N: = N + 1; go to 3°; 6° the number of errors is equal to N.

In realizing this algorithm it is possible to perform the calculations either in the field $GF(q^{mr})$ or in the field $GF(q^m)$. For running the algorithm it is necessary to perform multiplication in a finite field, then obtain the inverse quantity and perform the operation $\sigma x = x^{q^m}$.

6. Behavior of (L, g)-Codes for $n \to \infty$

In conclusion let us study the behavior of (L,g)-codes when $n \to \infty$ and the transmission rate k/n remains unchanged. Codes such that $d/n \to c \neq 0$ are called in this case "good" codes, whereas codes with $d/n \to 0$ are "bad." It is well known [5,6] that BCH codes, as well as all the codes that are invariant under an affine group of transformations, are "bad," whereas "good" codes can be obtained (as was shown by Zyablov [7]) by using the concatenation principle discovered by Forney [8]. (L,g)-codes also belong to "good" codes. For $n \to \infty$, most of them lie arbitrarily close to the Varshamov-Gilbert bound.

THEOREM 8. Let $L = GF(q^m)$, $n = q^m$, and let H(x) be the entropy. For any $0 < \lambda < 1$ and $\varepsilon > 0$ the probability that a randomly selected polynomial $g(z) \in L(z)$ of degree $[\lambda n/\log n]$ that has no roots in L will generate an (L,g)-code with parameters $k/n > 1 - H(d/n) - \varepsilon$ will tend to 1 with increasing n.

Proof. Let us denote by M_r a sphere of radius r in the space R_q (§ 2), i.e., a set of fractions in R of degree $\leq r$. Let N_r be the set of all the numerators of fractions in M_r, let V_r be the set of all normalized polynomials in L(z) of degree $t = [\lambda n/\log n]$ that do not have roots in L and are divisors of any polynomial in N_r, and let K be the set of all normalized polynomials in L(z) of degree t that do not have roots in L. By $\overline{A}$ we shall denote as usual the power of the set A.

Any polynomial belonging to K generates an (L,g)- code $C = \{\xi(z) \in R : \xi(z) \equiv 0 \bmod g(z)\}$ with a transmission rate $k/n \geq 1 - mt/n \geq 1 - \lambda$, and all $g(z) \in V_r$ generate codes of weight $\leq r$, whereas all $g(z) \in K - V_r$ generate codes of weight $> r$. Let us estimate the power of all these sets:

$$\overline{M}_r = \sum_{i=0}^{r} C_n^i (q-1)^i; \quad \overline{N}_r \leqslant \overline{M}_r; \quad \overline{V}_r < \overline{N}_r \cdot C_r^t;$$

$$\overline{K} = \sum_{i=0}^{t} C_n^i (-1)^i n^{t-i} \sim e^{-1} \cdot n^t \sim e^{-1} q^{\lambda n}$$

(as usual, $X(n) \sim Y(n)$ signifies that $X(n)/Y(n) \to 1$).

Let us determine μ by the condition $H(\mu) = \lambda - \varepsilon$, $0 < \mu < 1/2$ and write $r = \mu n$. All the $g(z) \in K - V_{\mu n}$ generate (L,g)-codes with parameters $H(d/n) > H(\mu) = \lambda - \varepsilon \geq 1 - k/n - \varepsilon$, and since

$$\overline{V}_{\mu n}/\overline{K} < C_{\mu n}^{\lambda n/\log n} \cdot q^{nH(\mu)} / e^{-1} q^{n\lambda} \to 0,$$

this completes the proof of the theorem.

Let us note that this result holds also for a narrower class of (L,g)-codes, namely for irreducible codes.

LITERATURE CITED

1. V. D. Goppa, "A new class of linear error-correcting codes," Probl. Peredachi Inform., 6, No. 3, 24-30 (1970).
2. E. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York (1968).
3. W. Milne, Numerical Calculus, Princeton Univ. Press, Princeton, N. J. (1949).
4. É. M. Gabidulin, "Decoding of maximal codes," Proceed. Third Conf. on the Theory of Information Transmission and Coding, Moscow–Uzhgorod (1967).
5. S. Lin and E. J. Weldon, "Long BCH codes are bad," Inform. and Control, 11, No. 10, 445-451 (1967).
6. T. Kasami, "An upper bound on k/n for affine–invariant codes with fixed d/n," IEEE Trans. Inform. Theory, 15, No. 1, 174-176 (1969).
7. V. V. Zyablov, "Estimation of complexity of construction of binary linear concatenated codes," Probl. Peredachi Inform., 7, No. 1, 5-13 (1971).
8. G. D. Forney, Concatenated Codes, MIT Press, Cambridge, Mass. (1966).